PATENT APPLICATION
Attorney Docket No. JP9200200207US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Akashi SATOH et al.	Examiner: DADA, Beemnet W.
Serial No: 10/730,773	Art Unit: 2135
Filed: December 9, 2003	
For: INFORMATION PROCESSING WITH DATA STORAGE	

APPEAL BRIEF

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The Appellants submit this brief pursuant to 37 C.F.R. §41.37(a)(1) in furtherance of the Notice of Appeal filed May 1, 2008.

Please charge Deposit Account 50-0510 the $510 fee for filing this Appeal Brief. No other fee is believed due with this Appeal Brief, however, should another fee be required please charge Deposit Account 50-0510.

Real Party in Interest

The real party in interest with respect to the present application is International Business Machines Corporation.

Related Appeals and Interferences

The Appellants' legal representative does not know of any other appeal, interference or judicial proceeding which will affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-25 are pending in the present application, with claims 1, 5, 7, 13, 17, 19, 22 and 23 being independent claims. Claims 1-25 are currently finally rejected and are the subject of this appeal.

Status of Amendments

No amendments to claims 1-25 were made after the Final Office Action dated January 2, 2008 ("FOA").

Summary of the Claimed Subject Matter

Claim 1 recites a data storage device for an information processing device. App., pp. 5, ll. 4-5; pp. 9, ll. 4-5; pp. 13, ll. 9-12; pp. 14, ll. 13-14, Fig. 1, item 100. The data storage device includes an encryption circuit for encrypting desired data and personal identification information by use of an encryption key created out of a given piece of the personal identification information. App., pp. 5, ll. 6-10; pp. 9, ll. 6-10; pp. 12, ll. 4-11; pp. 12, ll. 12-15; pp. 15, ll. 4-7, Fig. 1, item 54; pp. 17, ll. 12-21; pp. 18, ll. 16 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b; pp. 19, ll. 8-12, Fig. 2, items 1-a and 1-c; pp. 20, ll. 2-7, Fig. 3, items 2-a and 2-c. The data storage device further includes a recording medium for recording the data and the personal identification information encrypted by the encryption circuit. App., pp. 5, ll. 10-12; pp. 9, ll. 10-12; pp. 11, ll. 12-13; pp. 14, ll. 15-16, Fig. 1, item 10; pp. 19, ll. 1-2, Fig. 2, item 1-b; pp. 19, ll. 8-12, Fig. 2, item 1-c; pp. 20, ll. 2-7, Fig. 3, item 2-c. The data storage device further includes a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium. App., pp. 5, ll. 12-15; pp. 9, ll. 12-15; pp. 12, ll. 11-12; pp. 15, ll. 11-13, Fig. 1, item 58; pp. 17, ll. 21-28; pp. 19, ll. 15 to pp. 20, ll. 2, Fig. 3, items 2-a and 2-b. See also App., pp. 12, ll. 9-11 and pp. 18, ll. 16 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b.

Claim 2 is dependent on claim 1 and recites that the encryption circuit encrypts the encryption key by use of a different encryption key. App., pp. 9, ll. 16-17 and pp. 22, ll. 4-6, Fig. 5, item 4-b. Claim 2 further recites that the recording medium records the encryption key

encrypted by use of the different encryption key. App., pp. 9, ll. 16-18 and pp. 22, ll. 6-7, Fig. 5, item 4-c.

Claim 3 is dependent on claim 1 and recites that the recording medium includes a special storage area which is inaccessible in normal use. App., pp. 9, ll. 19-21 and pp. 31, ll. 19-21. Claim 3 further recites that the recording medium records the encryption key in the special storage area. App., pp. 9, ll. 18-21 and pp. 31, ll. 22-25.

Claim 4 is dependent on claim 1 and recites that the encryption circuit creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys. App., pp. 9, ll. 26-31; pp. 23, ll. 29 to pp. 24, ll. 3; pp. 24, ll. 8-13. See also pp. 17, ll. 21-28. Claim 4 further recites that the recording medium manages the storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys. App., pp. 9, ll. 30 to pp. 10, ll. 2 and pp. 24, ll. 3-13.

Claim 5 recites a data storage device for an information processing device. App., pp. 10, ll. 7-8 and pp. 13, ll. 9-12. The data storage device comprises an encryption circuit for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key created out of a given piece of the personal identification information. App., pp. 10, ll. 7-12; pp. 12, ll. 18-27; pp. 15, ll. 4-7, Fig. 1, item 54; pp. 17, ll. 17-21; pp. 18, ll. 16 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b; pp. 25, ll. 18-28, Fig. 7, items 6-a, 6-b and 6-c. The data storage device further comprises a recording medium for recording the data encrypted by use of the first encryption key, the first encryption key encrypted by use of the second encryption key, and the personal identification information encrypted by use of the second key. App., pp. 10, ll. 12-17; pp. 11, ll. 12-13; pp. 14, ll. 15-16, Fig. 1, item 10; pp. 17, ll. 17-21; pp. 25, ll. 18-28, Fig. 7, items 6-b and 6-c; pp. 27, ll. 6-12, Fig. 8, item 6-i. The data storage device further comprises a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium. App.,

pp. 10, ll. 17-19; pp. 15, ll. 11-13, Fig. 1, item 58; pp. 17, ll. 21-28; pp. 26, ll. 25 to pp. 27, ll. 3, Fig. 8, items 6-e, 6-f and 6-g. See also App., pp. 25, ll. 18-25, Fig. 2, items 6-a and 6-b.

Claim 7 recites a hard disk device. App., pp. 13, ll. 19-24; pp. 14, ll. 13-14, Fig. 1, item 100. The hard disk device includes a magnetic disk being a recording medium. App., pp. 5, ll. 18-19; pp. 11, ll. 12-13; pp. 14, ll. 15-16, Fig. 1, item 10. The hard disk device further includes a read-and-write mechanism for writing and reading data in and out of the magnetic disk. App., pp. 5, ll. 19-20; pp. 11, ll. 13-14; pp. 14, ll. 21-26, Fig. 1, items 20, 30 and 40. The hard disk device further includes a control mechanism (App., pp. 14, ll. 27-30, Fig. 1, items 50 and 60) having an encryption function for encrypting data to be written in the magnetic disk and for decrypting the encrypted data to be read out of the magnetic disk. App., pp. 5, ll. 20-23; pp. 11, ll. 14-17; pp. 15, ll. 4-7, Fig. 1, item 54. The control mechanism controls reading and writing the data by the reading-and-writing mechanism. App., pp. 5, ll. 23-25; pp. 11, ll. 17-18; pp. 14, ll. 27 to pp. 15, ll. 13. The control mechanism executes encryption of the data to be written in the magnetic disk for each unit of writing and reading data in and out of a storage area of the magnetic disk upon processing of writing the data in the magnetic disk, in response to turning on and off of the encryption mechanism. App., pp. 11, ll. 18-24 and pp. 33, ll. 26 to pp. 34, ll. 12. The encryption function of the control mechanism encrypts personal identification information by use of an encryption key created out of a given piece of the personal identification information. App., pp. 17, ll. 12-21 and pp. 18, ll. 16 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b.

Claim 8 is dependent on claim 7 and recites that the control mechanism judges as to whether the data are encrypted or not upon reading the data out of the storage medium, and further decrypts the data when the data are encrypted. App., pp. 11, ll. 27-30; pp. 31, ll. 1-10; pp. 36, ll. 13-23, Fig. 1, item 55.

Claim 10 is dependent on claim 7 and recites that the encryption function of the control mechanism encrypts desired data by use of the encryption key created out of a given piece of the personal identification information. App., pp. 17, ll. 12-16; pp. 18, ll. 16-28, Fig. 2, item 1-

a; pp. 19, ll. 8-12, Fig. 2, items 1-a and 1-c; pp. 20, ll. 2-7, Fig. 3, items 2-a and 2-c. Claim 10 further recites that the control mechanism executes user verification by use of the encrypted personal identification information. App., pp. 17, ll. 21-28 and pp. 19, ll. 15 to pp. 20, ll. 2, Fig. 3, items 2-a and 2-b. See also App., pp. 18, ll. 16 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b.

Claim 11 is dependent on claim 10 and recites that the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys. App., pp. 9, ll. 26-31; pp. 23, ll. 29 to pp. 24, ll. 3; pp. 24, ll. 8-13. See also pp. 17, ll. 21-28. Claim 11 further recites that the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys. App., pp. 9, ll. 30 to pp. 10, ll. 2 and pp. 24, ll. 3-13.

Claim 13 recites an information processing device. App., pp. 13, ll. 9-12; pp. 13, ll. 25-28, Fig. 18, item 200. The information processing device includes an operation control unit for executing various operation processing. App., pp. 13, ll. 28-31, Fig. 18, item 210 and pp. 14, ll. 4-7. The information processing device further includes a data storage device for storing data to be processed by the operation control unit. App., pp. 13, ll. 22-24 and pp. 14, ll. 2-8, Fig. 18, item 100. The data storage device includes an encryption function for encrypting desired data by use of a data encryption key and for encrypting personal identification information by use of a verification encryption key created out of a given piece of the personal identification information. App., pp. 15, ll. 4-7, Fig. 1, item 54; pp. 18, ll. 16 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b; pp. 25, ll. 18-28, Fig. 7, items 6-a, 6-b and 6-c. The data storage device executes user verification by use of the encrypted personal identification information. App., pp. 15, ll. 11-13, Fig. 1, item 58; pp. 26, ll. 25 to pp. 27, ll. 3, Fig. 8, items 6-e, 6-f and 6-g. See also App., pp. 25, ll. 18-25, Fig. 2, items 6-a and 6-b.

Claim 14 is dependent on claim 13 and recites that the data encryption key and the verification encryption are mutually identical.

App., pp. 25, ll. 10-13.

Claim 17 recites a data processing method for a data storage device for executing data writing and reading in and out of a recording medium of a data storage device. App., pp. 12, ll. 1-3. See also App., pp. 17, ll. 1-7. The data processing method for a data storage device includes the step of creating an encryption key out of a given piece of personal identification information. App., pp. 12, ll. 4-7; pp. 17, ll. 12-16; pp. 18, ll. 16-28, Fig. 2, item 1-a. The data processing method further includes the step of encrypting the personal identification information by use of the encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data. App., pp. 12, ll. 7-11; pp. 17, ll. 17-21; pp. 18, ll. 29 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b. The data processing method further includes the step of executing user verification based on the verification data recorded in the recording medium. App., pp. 12, ll. 11-12; pp. 17, ll. 21-28; pp. 19, ll. 15 to pp. 20, ll. 2, Fig. 3, items 2-a and 2-b. See also App., pp. 12, ll. 9-11 and pp. 18, ll. 16 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b. The data processing method further includes the step of executing any of encrypting write data transmitted from a host system by use of the encryption key and thereby recording the encrypted write data in the recording medium, and, decrypting the data read out of the recording medium by use of the encryption key and thereby transmitting the decrypted data to the host system. App., pp. 12, ll. 12-17; pp. 19, ll. 8-12, Fig. 2, items 1-a and 1-c; pp. 20, ll. 2-7, Fig. 3, items 2-a and 2-c.

Claim 18 is dependent on claim 17 and recites the step of encrypting the encryption key by use of a different encryption key and thereby recording the encrypted encryption key in the recording medium. App., pp. 22, ll. 4-7, Fig. 5, items 4-b and 4-c. See also App., pp. 14, ll. 15-16. Claim 18 further recites the step of decrypting the encrypted encryption key by use of the different encryption key and thereby decrypting the data read out of the recording medium by use of the decrypted encryption key. App., pp. 22, ll. 10-16, Fig. 5, items 4-e and 4-f.

Claim 19 recites a data processing method for a data storage device for executing data writing and reading in and out of a recording medium of

a data storage device. App., pp. 5, ll. 2-3; pp. 5, ll. 6-12; pp. 5, ll. 26-27. The data processing method for a data storage device includes the step of creating a verification encryption key out of a given piece of personal identification information. App., pp. 5, ll. 27-29; pp. 12, ll. 18-21; pp. 18, ll. 16-28, Fig. 2, item 1-a; pp. 25, ll. 18-20, Fig. 7, item 6-a. The data processing method further includes the step of encrypting the personal identification information by use of the verification encryption key and recording the encrypted personal identification information in the recording medium as verification data and further encrypting a data encryption key by use of the verification encryption key and thereby recording the encrypted data encryption key in the recording medium. App., pp. 5, ll. 29 to pp. 6, ll. 4; pp. 12, ll. 21-27; pp. 17, ll. 17-21; pp. 18, ll. 29 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b; pp. 25, ll. 21-28, Fig. 7, items 6-b and 6-c. The data processing method further includes the step of executing user verification based on the verification data recorded in the recording medium. App., pp. 6, ll. 5; pp. 12, ll. 27-28; pp. 17, ll. 21-28; pp. 26, ll. 25 to pp. 27, ll. 3, Fig. 8, items 6-e, 6-f and 6-g. See also App., pp. 5, ll. 31 to pp. 6, ll. 2; pp. 12, ll. 23-24; pp. 25, ll. 18-25, Fig. 2, items 6-a and 6-b. The data processing method further includes the step of decrypting the data encryption key recorded in the recording medium by use of the verification encryption key. App., pp. 6, ll. 6-7; pp. 12, ll. 28-30; pp. 27, ll. 3-6, Fig. 8, item 6-h. See also App., pp. 6, ll. 2-4 and pp. 12, ll. 26-27. The data processing method further includes the step of executing any of encrypting write data transmitted from a host system by use of the decrypted data encryption key and thereby recording the encrypted write data in the recording medium, and decrypting the data read out of the recording medium by use of the data encryption key and thereby transmitting the decrypted data to the host system. App., pp. 6, ll. 7-12; pp. 12, ll. 30 to pp. 13, ll. 4; pp. 27, ll. 6-12, Fig. 8, item 6-i.

Claim 20 is dependent on claim 19 and recites the step of decrypting the encrypted data encryption key recorded in the recording medium along with a change in the personal identification information by use of the verification encryption key created out of the personal identification information prior to the change, and then encrypting the data encryption

key again by use of the verification encryption key created out of the personal identification information after the change and thereby storing the data encryption key in the recording medium. App., pp. 27, ll. 26 to pp. 28, ll. 17, Fig. 9, items 6-j, 6-l, 6-m and 6-o. See also App., pp. 14, ll. 15-16.

Claim 21 is dependent on claim 19 and recites the step of decrypting the encrypted data encryption key recorded in the recording medium upon disabling encryption of the data recorded in the recording medium by use of the verification encryption key created out of the personal identification information prior to a change and thereby storing the decrypted data encryption key in the recording medium. App., pp. 30, ll. 6 to pp. 31, ll. 4, Fig. 11, items 7-a, 7-c and 7-d. See also App., pp. 14, ll. 15-16.

Claim 22 recites a program stored in computer readable memory for controlling a computer to control data writing and reading in and out of a magnetic disk. App., pp. 13, ll. 5-8; pp. 12, ll. 1-3; pp. 14, ll. 15-16. See also App., pp. 17, ll. 1-7. The program causing the computer to execute the process of creating an encryption key out of a given piece of personal identification information. App., pp. 12, ll. 4-7; pp. 17, ll. 12-16; pp. 18, ll. 16-28, Fig. 2, item 1-a. The program further causing the computer to execute the process of encrypting the personal identification information by use of the encryption key and thereby recording the encrypted personal identification information in the magnetic disk as verification data. App., pp. 12, ll. 7-11; pp. 17, ll. 17-21; pp. 18, ll. 29 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b. The program further causing the computer to execute the process of executing user verification based on the verification data recorded in the magnetic disk. App., pp. 12, ll. 11-12; pp. 17, ll. 21-28; pp. 19, ll. 15 to pp. 20, ll. 2, Fig. 3, items 2-a and 2-b. See also App., pp. 12, ll. 9-11 and pp. 18, ll. 16 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b. The program further causing the computer to execute the process of executing any of encrypting write data transmitted from a host system by use of the encryption key and thereby recording the encrypted write data in the magnetic disk, and decrypting the data read out of the magnetic disk by use of the encryption key and thereby transmitting the decrypted data to

the host system. App., pp. 12, ll. 12-17; pp. 19, ll. 8-12, Fig. 2, items 1-a and 1-c; pp. 20, ll. 2-7, Fig. 3, items 2-a and 2-c.

Claim 23 recites a program stored in computer readable memory for controlling a computer to control data writing and reading in and out of a magnetic disk. App., pp. 5, ll. 26-27; pp. 13, ll. 5-8; pp. 14, ll. 15-16. The program causing the computer to execute the process of creating an verification encryption key out of a given piece of personal identification information. App., pp. 5, ll. 27-29; pp. 12, ll. 18-21; pp. 18, ll. 16-28, Fig. 2, item 1-a; pp. 25, ll. 18-20, Fig. 7, item 6-a. The program further causing the computer to execute the process of encrypting the personal identification information by use of the verification encryption key and recording the encrypted personal identification information in the magnetic disk as verification data, and further encrypting a data encryption key by use of the verification encryption key and thereby recording the encrypted data encryption key in the magnetic disk. App., pp. 5, ll. 29 to pp. 6, ll. 4; pp. 12, ll. 21-27; pp. 17, ll. 17-21; pp. 18, ll. 29 to pp. 19, ll. 2, Fig. 2, items 1-a and 1-b; pp. 25, ll. 21-28, Fig. 7, items 6-b and 6-c. The program further causing the computer to execute the process of executing user verification based on the verification data recorded in the magnetic disk. App., pp. 6, ll. 5; pp. 12, ll. 27-28; pp. 17, ll. 21-28; pp. 26, ll. 25 to pp. 27, ll. 3, Fig. 8, items 6-e, 6-f and 6-g. See also App., pp. 5, ll. 31 to pp. 6, ll. 2; pp. 12, ll. 23-24; pp. 25, ll. 18-25, Fig. 2, items 6-a and 6-b. The program further causing the computer to execute the process of decrypting the data encryption key recorded in the magnetic disk by use of the verification encryption key. App., pp. 6, ll. 6-7; pp. 12, ll. 28-30; pp. 27, ll. 3-6, Fig. 8, item 6-h. See also App., pp. 6, ll. 2-4 and pp. 12, ll. 26-27. The program further causing the computer to execute the process of executing any of encrypting write data transmitted from a host system by use of the decrypted data encryption key and thereby recording the encrypted write data in the magnetic disk, and decrypting the data read out of the magnetic disk by use of the data encryption key and thereby transmitting the decrypted data to the host system. App., pp. 6, ll. 7-12; pp. 12, ll. 30 to pp. 13, ll. 4; pp. 27, ll. 6-12, Fig. 8, item 6-i.

Claim 24 is dependent on claim 7 and recites that the control mechanism writes the data in the recording medium without encrypting the data when the encryption function is turned off. App., pp. 16, ll. 27-31, Fig. 1, item 55 and pp. 36, ll. 17-23. See also App., pp. 14, ll. 27 to pp. 15, ll. 7.

Claim 25 is dependent on claim 17 and recites that the user verification comprises creating a candidate encryption key out of a given piece of candidate personal identification information. App., pp. 19, ll. 18-21, Fig. 3, item 2-a. The user verification further comprises creating candidate verification data by encrypting the candidate personal identification information by use of the candidate encryption key. App., pp. 19, ll. 21-24, Fig. 3, item 2-b. The user verification further comprises determining whether the candidate verification data are identical to the verification data previously recorded in the recording medium. App., pp. 19, ll. 24 to pp. 20, ll. 15.

Grounds for Rejection to be Reviewed on Appeal

I. Claims 1, 2, 5, 6, 13-23 and 25 are rejected under 35 U.S.C. §103 as being obvious over U.S. Patent Application Publication No. 2001/0056541 ("Matsuzaki") in view of U.S. Patent No. 5,604,800 issued to Johnson et al. ("Johnson").

II. Claim 3 is rejected under 35 U.S.C. §103 as being obvious over Matsuzaki in view of Johnson and further in view of U.S. Patent No. 7,062,652 issued to Hirota et al. ("Hirota").

III. Claim 4 is rejected under 35 U.S.C. §103 as being obvious over Matsuzaki in view of Johnson and further in view of European Patent Publication No. 0911738A2 ("Jackson").

IV. Claims 7-12 and 24 are rejected under 35 U.S.C. §103 as being obvious over Jackson in view of Johnson.

Argument

I. CLAIMS 1, 2, 5, 6, 13-23 AND 25 ARE NOT OBVIOUS OVER MATSUZAKI IN VIEW OF JOHNSON

"The identical invention must be shown in as complete detail as is contained in the ... claim." Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Furthermore, "[d]uring patent examination, the pending claims must be 'given their broadest reasonable interpretation consistent with the specification.' In re Hyatt, 21 1 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000)." MPEP, 2111 (emphasis added). Moreover, that "broadest reasonable interpretation of the claims must also be consistent with the interpretation that those skilled in the art would reach. In re Cortright, 165 F.3d 1353, 1359, 49 USPQ2d 1464, 1468 (Fed. Cir. 1999)." Id., (emphasis added).

Preliminary Comments

Responding to the points in the Amendment and Response to the Office Action dated July 6, 2007 ("Response"), the Examiner states, "In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references." FOA, pp. 2. The Examiner cites In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981) and In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986) as authority for this position. *Id.*

First, the Appellants do not attack the references individually, as alleged by the Examiner. In the Final Office Action, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system." The Appellants argue that "neither Matsuzaki nor Johnson express any appreciation of such alleged advantages." Response, pp. 19 (emphasis added). Thus, the Examiner's basic premise with regard to the Appellants' obviousness argument is refuted.

Second, in as much as the Examiner relies on the cited cases to rebut the Appellants' arguments that certain claim elements are not found in the cited art, the case holdings are taken out of context. In In re Keller, the sole issue regarding the prior art rejections was essentially whether the two applied references, viewed collectively, would have suggested the use of digital timing in a cardiac pacer to those of ordinary skill in the art at the time the invention was made. In re Keller, 231 USPQ at 880. An affidavit argued that one of the prior art references did not suggest combining digital timing to a known cardiac pacer. Id. Unlike the present case, the appellant in Keller did not argue a claim element alleged by the Examiner to be present in only a single prior art reference was missing from that reference.

In In re Merck & Co., the issue addressed by the court was whether motivation existed to combine the teachings of the prior art references. In re Merck & Co., 231 USPQ at 379. The appellant in Merck argued that one of the references teaches away from the claimed invention. Again, the court's holding is taken out of context since it did not address the situation where, contrary to the Examiner's determination, a claim element was not found in a cited prior art reference.

Claim 1

Claim 1 recites, in part, "an encryption circuit for encrypting desired data and personal identification information by use of an encryption key created out of a given piece of the personal identification information." Thus, claim 1 requires encrypting personal identification information by use of an encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the encryption key.

The Examiner alleges that paragraphs [0141] and [0152] of Matsuzaki teach an encryption circuit for encrypting desired data and

personal identification information by use of an encryption key. FOA, pp. 4.

The paragraph [0141] of Matsuzaki states:

> The encryption unit 102b, as the encryption unit 102, reads key information from the key storage medium 20, subjects the password received from the password input unit 101b to the encryption algorithm E1 using the read key information to generate an encrypted password, and writes the generated encrypted password as a file, to the storage unit 400b. Matsuzaki, para. [0141].

It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 1 requires encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraph [0152] of Matsuzaki states:

> The encryption unit 204b reads the key information from the key storage medium 20, receives the file key from the file key generation unit 201b. The encryption unit 204b then subjects the file key to the encryption algorithm E4 using the read key information as a key to generate a second encrypted file key, and writes the generated second encrypted file key to the header part of the encrypted file 404b in the storage unit 400b. It should be noted here that the encryption algorithm E4 complies with DES. Matsuzaki, para. [0152].

The Appellants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. FOA, pp. 5. The cited passage states:

> The step 804 of initializing the UAS 12 with recognition and comprehension data is shown in greater detail in FIG. 4b. As shown in FIG. 4b, processor 30 starts the data initialization

> process by prompting 810 the user for a dynamic personal identification number (DPIN) or code. This DPIN may be any desired alpha-numeric which the user wants to use as an identification code. Step 810 is preferably carried out by sending a user prompt to the display subsystem 50 and soliciting a response from the user via the keyboard subsystem 52. Once a DPIN is received from the keyboard subsystem 52, processor 30 proceeds to generate 814 a master hash code and a master key code using the DPIN as input. As will be explained later, this master key code is used to encrypt information stored on the master EKE 70. Preferably, processor 30 generates the master key code in two steps. First, processor 30 executes the hash code generation logic stored in section 62 of the non-volatile memory 38, using the DPIN as input, to generate a master hash code. Processor 30 preferably generates the master hash code by implementing a hashing algorithm. In the preferred embodiment . . . . Johnson, col. 10, ll. 46-66.

The Appellants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating an encryption key out of a piece of the personal identification information. As previously noted, claim 1 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the encryption key.

Additionally, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system." FOA, pp. 5. The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

Furthermore, in the Response to Arguments section, the Examiner alleges:

> In this case, Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password

> using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. FOA, pp. 2-3.

The Appellants respectfully submit that even assuming *arguendo* that it would be obvious to combine the teachings of Johnson within the system of Matsuzaki, the combination nonetheless fails to teach or suggest encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information as required by claim 1. Even if personal identification information is encrypted by use of an encryption key as allegedly disclosed by Matsuzaki, and even if said encryption key is created out of a given piece of personal identification information as allegedly disclosed by Johnson, it does not inherently follow that the personal identification information which is encrypted is the same as the personal identification information out of which the encryption key is created. As previously noted, claim 1 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the encryption key.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 1. The Appellants submit that the rejection of claim 1 is in error and respectfully request that the rejection of claim 1 be reversed by the honorable Board.

Claim 2

Claim 2 is dependent on claim 1 and recites, "The data storage device according to claim 1, wherein the encryption circuit encrypts the encryption key by use of a different encryption key, and the recording medium records the encryption key encrypted by use of the different encryption key." It is evident from antecedent basis that the encryption key recited in claim 2 is the same encryption key that was recited in claim 1.

The Examiner alleges that paragraphs [0148] through [0152] of Matsuzaki teach the limitations introduced by claim 2. FOA, pp. 9. The passage cited by the Examiner states:

> The encryption unit 203b then subjects a plaintext included in the plaintext file 401b to the encryption algorithm E3 using the received file key as a key to generate a ciphertext, and writes an encrypted file 404b including the generated ciphertext in the data part thereof, to the storage unit 400.
>
> (7) Encryption Unit 202b
>
> The encryption unit 202b receives the password from the decryption unit 205b and the file key from the file key generation unit 201b. The encryption unit 202b then subjects the received file key to the encryption algorithm E2 using the received password as a key to generate a first encrypted file key, and writes the generated first encrypted file key to the header part of the encrypted file 404b in the storage unit 400b.
>
> (8) Encryption Unit 204b
>
> The encryption unit 204b reads the key information from the key storage medium 20, receives the file key from the file key generation unit 201b. The encryption unit 204b then subjects the file key to the encryption algorithm E4 using the read key information as a key to generate a second encrypted file key, and writes the generated second encrypted file key to the header part of the encrypted file 404b in the storage unit 400b. It should be noted here that the encryption algorithm E4 complies with DES. Matsuzaki, para. [0148]-[0152].

In regards to claim 1, the Examiner alleges that "encrypting file key using read key" teaches encrypting desired data by use of an encryption key as required by claim 1. FOA, pp. 4. The Appellants interpret "read key" to refer to the read key information from the key storage medium, as the language "read key" is not used in any other context in paragraphs [0148] through [0152] of Matsuzaki. It follows from this statement that the Examiner is alleging the read key of Matsuzaki to be equivalent to the encryption key of claim 1.

As noted above, the encryption key of claim 2 is the same as the encryption key of claim 1. Therefore, Matsuzaki cannot teach claim 2 unless the read key information of Matsuzaki is equivalent to the encryption key of claim 2. It follows that Matsuzaki, alone or in combination with other teachings, cannot teach claim 2 unless the

read key information is encrypted by use of a different encryption key.

The Appellants submit that the cited passage of Matsuzaki fails to teach or suggest encrypting the read key information by use of a different encryption key. The passage teaches that a plaintext and a file key are encrypted. However, this fails to teach or suggest claim 2 because the plaintext and the file key are clearly not equivalent to the read key information.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 2. The Appellants submit that the rejection of claim 2 is in error and respectfully request that the rejection of claim 2 be reversed by the honorable Board.

Claim 5

Claim 5 recites, in part, "an encryption circuit for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key created out of a given piece of the personal identification information." Thus, claim 5 requires encrypting personal identification information by use of a second encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the second encryption key.

The Examiner alleges that paragraphs [0141], [0147], [0148] and [0152] of Matsuzaki teach an encryption circuit for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key. FOA, pp. 5. After careful review of Matsuzaki, the Appellants respectfully disagree with this interpretation.

The paragraph [0141] of Matsuzaki states:

> The encryption unit 102b, as the encryption unit 102, reads key information from the key storage medium 20, subjects the password

> received from the password input unit 101b to the encryption algorithm E1 using the read key information to generate an encrypted password, and writes the generated encrypted password as a file, to the storage unit 400b. Matsuzaki, para. [0141].

It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 5 requires encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraphs [0147] and [0148] of Matsuzaki state:

> The encryption unit 203b, as the encryption unit 203, reads the plaintext file 401b from the storage unit 400b, and receives the file key from the file key generation unit 201b.
>
> The encryption unit 203b then subjects a plaintext included in the plaintext file 401b to the encryption algorithm E3 using the received file key as a key to generate a ciphertext, and writes an encrypted file 404b including the generated ciphertext in the data part thereof, to the storage unit 400. Matsuzaki, para. [0147]-[0148].

It is clear from this passage that the plaintext read from the storage unit and the file key received from the file key storage unit are used to generate a ciphertext. However, paragraphs [0147] and [0148] make no mention of encrypting personal identification information. The cited passage therefore clearly fails to teach the limitation of claim 5 requiring encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information.

The paragraph [0152] of Matsuzaki states:

> The encryption unit 204b reads the key information from the key storage medium 20, receives the file key from the file key generation unit 201b. The encryption unit 204b then subjects the file key to the encryption algorithm E4 using the read key information as a key to generate a second encrypted file key, and writes the generated second encrypted file key to the header part of the encrypted file 404b in the storage unit 400b. It should be

> noted here that the encryption algorithm E4 complies with DES. Matsuzaki, para. [0152].

The Appellants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. FOA, pp. 6. The cited passage is reproduced above in regards to claim 1. The Appellants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating a second encryption key out of a piece of the personal identification information. As previously noted, claim 5 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the second encryption key.

Additionally, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system." FOA, pp. 6. The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

Furthermore, in the Response to Arguments section, the Examiner alleges:

> In this case, Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an

> encryption key out of a given piece of personal identification information [column 10, lines 48-65]. FOA, pp. 2-3.

The Appellants respectfully submit that even assuming *arguendo* that it would be obvious to combine the teachings of Johnson within the system of Matsuzaki, the combination nonetheless fails to teach or suggest encrypting personal identification information by use of a second encryption key created out of a given piece of the personal identification information as required by claim 5. Even if personal identification information is encrypted by use of an encryption key as allegedly disclosed by Matsuzaki, and even if said encryption key is created out of a given piece of personal identification information as allegedly disclosed by Johnson, it does not inherently follow that the personal identification information which is encrypted is the same as the personal identification information out of which the encryption key is created. As previously noted, claim 5 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the second encryption key.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 5. The Appellants submit that the rejection of claim 5 is in error and respectfully request that the rejection of claim 5 be reversed by the honorable Board.

Claim 6

Claim 6 is dependent on and further limits claim 5. Since the rejection of claim 5 is believed in error, the rejection of claim 6 is also believed in error for at least the same reasons as claim 5.

Claim 13

Claim 13 recites, in part, "wherein the data storage device includes an encryption function for encrypting desired data by use of a data encryption key and for encrypting personal identification information by use of a verification encryption key created out of a given piece of the personal identification information." Thus, claim 13 requires encrypting personal identification information by use of

a verification encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the verification encryption key.

The Examiner alleges that paragraphs [0141] and [0152] of Matsuzaki teach a data storage device including an encryption function for encrypting desired data by use of a data encryption key and for encrypting personal identification information by use of a verification encryption key. FOA, pp. 6.

The paragraph [0141] of Matsuzaki is recited above in regards to claim 1. It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 13 requires encrypting personal identification information by use of a verification encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraph [0152] of Matsuzaki is also recited above in regards to claim 1. The Appellants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. FOA, pp. 7. The cited passage is reproduced above in regards to claim 1. The Appellants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating a verification encryption key out of a piece of the personal identification information. As previously noted, claim 13 requires that the personal identification information which is encrypted is the same as

the personal identification information of which a given piece was used to create the verification encryption key.

Additionally, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system." FOA, pp. 7. The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

Furthermore, in the Response to Arguments section, the Examiner alleges:

> In this case, Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. FOA, pp. 2-3.

The Appellants respectfully submit that even assuming *arguendo* that it would be obvious to combine the teachings of Johnson within the system of Matsuzaki, the combination nonetheless fails to teach or suggest encrypting personal identification information by use of a verification encryption key created out of a given piece of the personal identification information as required by claim 13. Even if personal identification information is encrypted by use of an encryption key as allegedly disclosed by Matsuzaki, and even if said encryption key is created out of a given piece of personal identification information as allegedly disclosed by Johnson, it does not inherently follow that the personal identification information which is encrypted is the same as the personal identification information out of which the encryption key is created. As previously noted, claim 13 requires that the personal identification

information which is encrypted is the same as the personal identification information of which a given piece was used to create the verification encryption key.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 13. The Appellants submit that the rejection of claim 13 is in error and respectfully request that the rejection of claim 13 be reversed by the honorable Board.

Claim 14

Claim 14 is dependent on claim 13 and recites, "The information processing device according to claim 13, wherein the data encryption key and the verification encryption are mutually identical." It is evident from antecedent basis that the data encryption key and the verification encryption key recited in claim 14 are the same data encryption key and verification encryption key that were recited in claim 13.

Claim 14 is rejected under the same rationale as claim 13. FOA, pp. 6-7. Thus, the reasons provided above as to why claim 13 is allowable apply equally to claim 14.

Additionally, in regards to claim 13, the Examiner alleges that "encrypting plaintext file using file key" teaches encrypting desired data by use of a data encryption key as required by claim 13. FOA, pp. 6. The Examiner further alleges that "encrypting password using read key" teaches encrypting personal identification information by use of a verification encryption key as required by claim 13. FOA, pp. 6. The "read key" refers to the read key information from the key storage medium, as the language "read key" is not used in any other context in paragraphs [0141] and [0152] of Matsuzaki. It follows from these statements that the Examiner is alleging the file key disclosed by Matsuzaki to be equivalent to the data encryption key of claim 13 and the read key of Matsuzaki to be equivalent to the verification encryption key of claim 13. It follows that Matsuzaki, alone or in combination with other teachings, cannot teach claim 14

unless the file key and the read key information are mutually identical.

The Appellants respectfully submit that Matsuzaki does not teach or suggest that the file key and the read key are mutually identical. To the contrary, Matsuzaki discloses: "The file key generation unit 201b, as the file key generation unit 201, generates a file key, and outputs the generated file key to the encryption unit 202b, the encryption unit 203b, and the encryption unit 204b." Matsuzaki, para. [0143]. It is thus evident that the file key disclosed by Matsuzaki is generated by a file key generation unit. Matsuzaki additionally discloses, "The encryption unit 102b, as the encryption unit 102, reads key information from the key storage medium 20, subjects the password received from the password input unit 101b to the encryption algorithm E1 using the read key information to generate an encrypted password, and writes the generated encrypted password as a file, to the storage unit 400b." Matsuzaki, para. [0141]. It is thus evident that the read key information disclosed by Matsuzaki is read from a key storage medium. Furthermore, it is evident from fig. 10 of Matsuzaki that the file key generation unit (num. 201b) and the key storage medium (num. 20) are distinct. The fact that the file key and the read key information are generated or retrieved from distinct units suggests that the file key and the read key information are generally not mutually identical.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 14. The Appellants submit that the rejection of claim 14 is in error and respectfully request that the rejection of claim 14 be reversed by the honorable Board.

Claims 15 and 16

Claim 15 and 16 are dependent on and further limit claim 13. Since the rejection of claim 13 is believed in error, the rejection of claims 15 and 16 are also believed in error for at least the same reasons as claim 13.

Claim 17

Claim 17 recites, in part, "creating an encryption key out of a given piece of personal identification information; encrypting the personal identification information by use of the encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data." Thus, claim 17 requires encrypting personal identification information by use of an encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the encryption key.

The Examiner alleges that paragraphs [0141] and [0152] of Matsuzaki teach encrypting personal identification information by use of an encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data. FOA, pp. 7.

The paragraph [0141] of Matsuzaki is recited above in regards to claim 1. It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 17 requires encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraph [0152] of Matsuzaki is also recited above in regards to claim 1. The Appellants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that column 10, lines 48-65 of Johnson teach creating an encryption key out of a given piece of personal identification information. FOA, pp. 8. The cited passage

is reproduced above in regards to claim 1. The Appellants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating an encryption key out of a piece of the personal identification information. As previously noted, claim 17 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the encryption key.

Additionally, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of Matsuzaki in order to enhance the security of the system." FOA, pp. 8. The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

Furthermore, in the Response to Arguments section, the Examiner alleges:

> In this case, Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. FOA, pp. 2-3.

The Appellants respectfully submit that even assuming *arguendo* that it would be obvious to combine the teachings of Johnson within the system of Matsuzaki, the combination nonetheless fails to teach or suggest encrypting personal identification information by use of an encryption key created out of a given piece of the personal identification information as required by claim 17. Even if personal identification information is encrypted by use of an encryption key as allegedly disclosed by Matsuzaki, and even if said encryption key

is created out of a given piece of personal identification information as allegedly disclosed by Johnson, it does not inherently follow that the personal identification information which is encrypted is the same as the personal identification information out of which the encryption key is created. As previously noted, claim 17 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the encryption key.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 17. The Appellants submit that the rejection of claim 17 is in error and respectfully request that the rejection of claim 17 be reversed by the honorable Board.

Claim 18

Claim 18 is dependent on claim 17 and recites, in part, "encrypting the encryption key by use of a different encryption key and thereby recording the encrypted encryption key in the recording medium." It is evident from antecedent basis that the encryption key recited in claim 18 is the same encryption key that was recited in claim 17.

The Examiner alleges that paragraphs [0148] through [0152] of Matsuzaki teaches this limitation of claim 18. FOA, pp. 10. The passage cited by the Examiner is reproduced above in regards to claim 2.

In regards to claim 17, the Examiner alleges that "encrypting password using read key and storing the encrypted password" teaches the limitation of claim 17 requiring encrypting personal identification information by use of an encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data. FOA, pp. 7. The "read key" refers to the read key information from the key storage medium, as the language "read key" is not used in any other context in paragraphs [0148] through [0152] of Matsuzaki. It follows from these statements that the Examiner is alleging the read key disclosed by

Matsuzaki to be equivalent to the encryption key of claim 17. Furthermore, as previously noted, the encryption key of claim 18 is the same as the encryption key of claim 17. Therefore, Matsuzaki cannot teach claim 18 unless the read key information of Matsuzaki is equivalent to the encryption key of claim 18. It follows that Matsuzaki, alone or in combination with other teachings, cannot teach claim 18 unless the read key information is encrypted by use of a different encryption key.

The Appellants respectfully submit that the cited passage of Matsuzaki fails to teach or suggest encrypting the read key information by use of a different encryption key. The passage teaches that a plaintext and a file key are encrypted. However, this fails to teach or suggest claim 18 because the plaintext and the file key are clearly not equivalent to the read key information.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 18. The Appellants submit that the rejection of claim 18 is in error and respectfully request that the rejection of claim 18 be reversed by the honorable Board.

Claim 19

Claim 19 recites, in part, "creating a verification encryption key out of a given piece of personal identification information; encrypting the personal identification information by use of the verification encryption key and recording the encrypted personal identification information in the recording medium as verification data, and further encrypting a data encryption key by use of the verification encryption key and thereby recording the encrypted data encryption key in the recording medium." Thus, claim 19 requires encrypting personal identification information by use of a verification encryption key. Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the verification encryption key.

The Examiner alleges that paragraphs [0141] and [0152] of Matsuzaki teach encrypting a personal identification information by use of a verification encryption key and recording the encrypted personal identification information in the recording medium as verification data. FOA, pp. 8.

The paragraph [0141] of Matsuzaki is recited above in regards to claim 1. It is clear from this passage that the key information from the key storage medium and the password received from the password input unit are used to generate an encrypted password. By contrast, claim 19 requires encrypting personal identification information by use of a verification encryption key created out of a given piece of the personal identification information. Paragraph [0141] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The paragraph [0152] of Matsuzaki is also recited above in regards to claim 1. The Appellants respectfully submit that paragraph [0152] makes no mention of encrypting personal identification information and using a piece of the personal identification information as an encryption key.

The Examiner further alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. FOA, pp. 9. The cited passage is reproduced above in regards to claim 1. The Appellants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating a verification encryption key out of a piece of the personal identification information. As previously noted, claim 19 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the verification encryption key.

Additionally, the Examiner argues, "It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Johnson within the system of

Matsuzaki in order to enhance the security of the system." FOA, pp. 9. The Office Action, however has not explained, and it not evident, how employing the teachings of Johnson within the system of Matsuzaki enhances the security of the system. The Office Action has also not explained why a person of ordinary skill in the art would have found it obvious to reconstruct Matsuzaki to "enhance the security of the system." In this regard, neither Matsuzaki nor Johnson express any appreciation of such alleged advantages.

Furthermore, in the Response to Arguments section, the Examiner alleges:

> In this case, Matsuzaki teaches an encryption circuit (i.e., encryption units E1-E4) for encrypting desired data (i.e., encrypting file key using read key) and personal identification information by use of an encryption key (i.e., encrypting password using read key) [paragraphs 0141 and 0152]. Further, Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. FOA, pp. 2-3.

The Appellants respectfully submit that even assuming *arguendo* that it would be obvious to combine the teachings of Johnson within the system of Matsuzaki, the combination nonetheless fails to teach or suggest encrypting personal identification information by use of a verification encryption key created out of a given piece of the personal identification information as required by claim 19. Even if personal identification information is encrypted by use of an encryption key as allegedly disclosed by Matsuzaki, and even if said encryption key is created out of a given piece of personal identification information as allegedly disclosed by Johnson, it does not inherently follow that the personal identification information which is encrypted is the same as the personal identification information out of which the encryption key is created. As previously noted, claim 19 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the verification encryption key.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of

obviousness for claim 19. The Appellants submit that the rejection of claim 19 is in error and respectfully request that the rejection of claim 19 be reversed by the honorable Board.

Claim 20

Claim 20 is dependent on claim 19 and recites, "The data processing method for a data storage device according to claim 19, further comprising the step of: decrypting the encrypted data encryption key recorded in the recording medium along with a change in the personal identification information by use of the verification encryption key created out of the personal identification information prior to the change, and then encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change and thereby storing the data encryption key in the recording medium." It is evident from antecedent basis that the data encryption key, the verification encryption key and the personal identification information recited in claim 20 are the same data encryption key, verification encryption key and personal identification information that were recited in claim 19.

In regards to claim 19, the Examiner alleges that "the Examiner alleges that "encrypting password using read key and storing the encrypted password" teaches encrypting a personal identification information by use of a verification encryption key and recording the encrypted personal identification information in the recording medium as verification data. FOA, pp. 8. The Examiner further alleges that "encrypting file key by using read key" teaches encrypting a data encryption key by use of the verification encryption key. *Id.* The "read key" refers to the read key information from the key storage medium, as the language "read key" is not used in any other context in paragraphs [0141] and [0152] of Matsuzaki. It follows from these statements that the Examiner is alleging the file key of Matsuzaki to be equivalent to the data encryption key of claim 19, the read key of Matsuzaki to be equivalent to the verification encryption key of claim 19 and the password of Matsuzaki to be equivalent to the personal identification information of claim 19. Furthermore, as

previously noted, it is evident from antecedent basis that the data encryption key, the verification encryption key and the personal identification information of claim 20 are the same as the corresponding elements of claim 19. Therefore, Matsuzaki cannot teach claim 20 unless the file key of Matsuzaki is equivalent to the data encryption key of claim 20, the read key information of Matsuzaki is equivalent to the verification encryption key of claim 20 and the password of Matsuzaki is equivalent to the personal identification information of claim 20.

The Examiner alleges that paragraphs [0192] through [0199] of Matsuzaki teach claim 20. FOA, pp. 10. After careful review of Matsuzaki, the Appellants respectfully disagree with this interpretation.

Paragraphs [0192] and [0193] of Matsuzaki state:

> (2) The following is an explanation of the operation of the file management apparatus 10b when a password is changed, with reference to a flowchart shown in FIG. 14.
>
> The password registration unit 100b reads key information from the key storage medium 20, reads a second encrypted file key from the encrypted file 404b, and subjects the second encrypted file key to the decryption algorithm D4 using the key information as a key to generate a file key (step S261). Following this, the password registration unit 100b receives an input of a new password from the user (step S262), subjects the generated file key to the encryption algorithm E2 using the new password as a key to generate a new first encrypted file key (step S263), and updates the first encrypted file key in the encrypted file 404b to the new first encrypted file key (step S264). Matsuzaki, para. [0192]-[0193].

The cited passage teaches that a file key is encrypted "using the new password as a key". However, the password disclosed by Matsuzaki is clearly not equivalent to the verification encryption key of claim 20. Therefore, the cited passage clearly fails to teach or suggest encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change as is required by claim 20.

Paragraph [0194] of Matsuzaki states:

> (4) The following is an explanation of the operation of the file management apparatus 10b when key information is updated, with reference to a flowchart shown in FIG. 15. Matsuzaki, para. [0194].

The Appellants respectfully submit that the cited passage clearly fails to teach or suggest encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change as is required by claim 20.

Paragraphs [0195] through [0197] of Matsuzaki states:

> (4) The following is an explanation of the operation of the file management apparatus 10b when key information is updated, with reference to a flowchart shown in FIG. 15.
>
> The key storage medium stores new key information beforehand, instead of the key information employed previously (referred to as old key information).
>
> The file encryption unit 200b receives an input of a password that is the same as the password received previously (step S281), reads a first encrypted file key from the encrypted file 404b (step S282), and subjects the first encrypted file key to the decryption algorithm D2 using the received password as a key to generate a file key (step S283). Following this, the file encryption unit 200b reads the new key information from the key storage medium, subjects the file key to the encryption algorithm E4 using the new key information as a key to generate a new second encrypted file key (step S284), and updates the second encrypted file key in the encrypted file 404b to the new second encrypted file key (step S285). Matsuzaki, para. [0195]-[0197] (emphasis added.)

The cited passage clearly teaches that the password is the same as the password received previously. As previously noted, Matsuzaki cannot teach claim 20 unless the password of Matsuzaki is equivalent to the personal identification information of claim 20. However, claim 20 requires a "verification encryption key created out of the personal identification information prior to the change" and further requires a "verification encryption key created out of the personal identification information after the change." It is clearly impossible to fulfill either requirement of claim 20 if no change to the personal identification information occurs.

Paragraphs [0198] and [0199] of Matsuzaki state:

> (5) In the above embodiment, the encrypted password is stored in a computer system in which a plaintext has been encrypted to generate a ciphertext, and so decryption of the ciphertext using a password is made only possible within the computer system. To enable the decryption of the ciphertext using the password in another computer system, the encrypted key may be stored in a portable storage medium, and inputted into the other computer system.
>
> Here, the password registration unit 100b in the computer system writes the encrypted password to a portable storage medium such as a SD memory card. Also, the user writes the encrypted file to another portable storage medium. The user then loads the portable storage medium to which the encrypted key has been written, and the portable storage medium to which the encrypted file has been written, on the other computer system, so that a file decryption unit in the other computer system reads the encrypted key from the portable storage medium, decrypts the read encrypted key, and also, reads the encrypted file from the portable storage medium, and decrypts the read encrypted file. Matsuzaki, para. [0198]-[0199].

The Appellants respectfully submit that the cited passage clearly fails to teach or suggest encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change as is required by claim 20.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 20. The Appellants submit that the rejection of claim 20 is in error and respectfully request that the rejection of claim 20 be reversed by the honorable Board.

Claim 21

Claim 21 is dependent on claim 19 and recites, "The data processing method for a data storage device according to claim 19, further comprising the step of: decrypting the encrypted data encryption key recorded in the recording medium upon disabling encryption of the data recorded in the recording medium by use of the verification encryption key created out of the personal identification information prior to a change and thereby storing the decrypted data encryption key in the recording medium." It is

emphasized that claim 21 requires storing a decrypted data encryption key in a recording medium.

The Examiner alleges that paragraphs [0192] through [0199] of Matsuzaki teach claim 21. FOA, pp. 10-11. Paragraphs [0192] through [0199] of Matsuzaki are recited above in regards to claim 20.

The Appellants respectfully submit that the passage cited by the Examiner fails to teach or suggest storing a decrypted encryption key in a recording medium as is required by claim 21. To the contrary, the cited passage appears to teach encrypting the recorded encryption key in all cases where an encryption key is recorded in a recording medium.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 21. The Appellants submit that the rejection of claim 21 is in error and respectfully request that the rejection of claim 21 be reversed by the honorable Board.

Claim 22

Claim 22 is rejected under the same rationale as claim 17. FOA, pp. 7-8. Thus, the reasons cited above as to why claim 17 is allowable apply equally to claim 22.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 22. The Appellants submit that the rejection of claim 22 is in error and respectfully request that the rejection of claim 22 be reversed by the honorable Board.

Claim 23

Claim 23 is rejected under the same rationale as claim 19. FOA, pp. 8-9. Thus, the reasons cited above as to why claim 19 is allowable apply equally to claim 23.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 23. The Appellants submit that the rejection

of claim 23 is in error and respectfully request that the rejection of claim 23 be reversed by the honorable Board.

Claim 25

Claim 25 is dependent on claim 17 and recites, in part, "creating a candidate encryption key out of a given piece of candidate personal identification information." Claim 25 further recites, in part, "creating candidate verification data by encrypting the candidate personal identification information by use of the candidate encryption key." Thus, claim 25 requires encrypting candidate personal identification information by use of a candidate encryption key. Furthermore, it is evident from antecedent basis that the candidate personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the candidate encryption key.

In rejecting claim 25, the Examiner alleges,

> As per claim 25, Matsuzaki further teaches for executing user verification by use of the encrypted personal identification information stored in the recording medium (i.e., the encrypted password is decrypted and used as an encryption key to encrypt a file key) [paragraphs 0145 & 0150], further the user inputs the password for decrypting the encrypted file key [paragraphs 0156-0159]). Further Johnson teaches a personal authentication device, including creating an encryption key out of a given piece of personal identification information [column 10, lines 48-65]. FOA, pp. 11.

After careful review of Matsuzaki, the Appellants respectfully disagree with this interpretation. Paragraph [0145] of Matsuzaki states,

> The decryption unit 205b reads the encrypted password stored in the storage unit 400b, and reads the key information from the key storage medium 20. The decryption unit 205b then subjects the read encrypted password to the decryption algorithm D1 using the read key information to generate a password, and outputs the generated password to the encryption unit 202b. Matsuzaki, para. [0145].

The Appellants respectfully submit that paragraph [0145] fails to disclose encrypting candidate personal identification information and creating a candidate encryption key out of a piece of the candidate personal identification information.

Paragraph [0150] of Matsuzaki states,

> The encryption unit 202b receives the password from the decryption unit 205b and the file key from the file key generation unit 201b. The encryption unit 202b then subjects the received file key to the encryption algorithm E2 using the received password as a key to generate a first encrypted file key, and writes the generated first encrypted file key to the header part of the encrypted file 404b in the storage unit 400b. Matsuzaki, para. [0150].

The Appellants respectfully submit that Matsuzaki fails to disclose that the file key comprises candidate personal identification information. Therefore, encrypting the file key disclosed by Matsuzaki cannot teach or suggest encrypting candidate personal identification information and creating a candidate encryption key out of a piece of the candidate personal identification information as required by claim 25. As previously noted, claim 25 requires that the candidate personal identification information which is encrypted is the same as the candidate personal identification information of which a given piece was used to create the candidate encryption key.

Paragraphs [0156]-[0159] of Matsuzaki state,

> (10) Password Input Unit 301b
>
> The password input unit 301b, as the password input unit 101, receives an input of a password from the user, and outputs the received password to the decryption unit 302b.
>
> (11) Decryption Unit 302b
>
> The decryption unit 302b receives the password from the password input unit 301b, reads the first encrypted file key included in the header part of the encrypted file 404b in the storage unit 400b. The decryption unit 302b then subjects the read first encrypted file key to the decryption algorithm D2 using the read password as a key to generate a file key, and outputs the generated file key to the switch unit 303b. Matsuzaki, para. [0156]-[0159].

The Appellants respectfully submit paragraphs [0156] through [0159] do not disclose encryption. Therefore, paragraphs [0156] through [0159] of Matsuzaki cannot teach encrypting candidate personal identification information and creating a candidate

encryption key out of a piece of the candidate personal identification information as required by claim 25.

Furthermore, as previously noted, Matsuzaki fails to state that the file key comprises candidate personal identification information. Therefore, even assuming *arguendo* that an encryption process which reverses the decryption process disclosed in paragraphs [0156] through [0159] is performed, such an encryption process nonetheless cannot be equivalent to encrypting candidate personal identification information and creating a candidate encryption key out of a piece of the candidate personal identification information.

The Examiner further alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. FOA, pp. 5. The cited passage states:

> The step 804 of initializing the UAS 12 with recognition and comprehension data is shown in greater detail in FIG. 4b. As shown in FIG. 4b, processor 30 starts the data initialization process by prompting 810 the user for a dynamic personal identification number (DPIN) or code. This DPIN may be any desired alpha-numeric which the user wants to use as an identification code. Step 810 is preferably carried out by sending a user prompt to the display subsystem 50 and soliciting a response from the user via the keyboard subsystem 52. Once a DPIN is received from the keyboard subsystem 52, processor 30 proceeds to generate 814 a master hash code and a master key code using the DPIN as input. As will be explained later, this master key code is used to encrypt information stored on the master EKE 70. Preferably, processor 30 generates the master key code in two steps. First, processor 30 executes the hash code generation logic stored in section 62 of the non-volatile memory 38, using the DPIN as input, to generate a master hash code. Processor 30 preferably generates the master hash code by implementing a hashing algorithm. In the preferred embodiment . . . . Johnson, col. 10, ll. 46-66.

The Appellants submit that column 10, lines 48-65 of Johnson do not disclose encrypting candidate personal identification information and creating a candidate encryption key out of a piece of the candidate personal identification information. As previously noted, claim 25 requires that the candidate personal identification information which is encrypted is the same as the candidate personal

identification information of which a given piece was used to create the candidate encryption key.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 25. The Appellants submit that the rejection of claim 25 is in error and respectfully request that the rejection of claim 25 be reversed by the honorable Board.

II. CLAIM 3 IS NOT OBVIOUS OVER MATSUZAKI IN VIEW OF JOHNSON AND FURTHER IN VIEW OF HIROTA

Claim 3

Claim 3 is dependent on claim 1 and recites, "The data storage device according to claim 1, wherein the recording medium includes a special storage area which is inaccessible in normal use, and the recording medium records the encryption key in the special storage area."

In rejecting claim 3, the Examiner alleges that "Hirota teaches a recording medium includes a special storage area which is inaccessible in normal use, and the recording medium records the encryption key in the special storage area [see for example, column 12, lines 49-54 and column 10, lines 22-36]." FOA, pp. 11.

The Examiner argues that the cited claim elements are found in Hirota by merely copying the claim elements and citing column and line numbers of Hirota in brackets. The rejection does not provide a comprehensive explanation of why the Examiner considers the limitations of claim 3 disclosed in Hirota. The Appellants respectfully submit that the Examiner has failed to clearly articulate a detailed explanation of disclosed structures relied upon in Hirota in accordance with 37 CFR 1.104(c)(2). Therefore, the Appellants respectfully submit that the Examiner has not met the burden of proof required to demonstrate obviousness.

The first passage cited by the Examiner states:

> The authentication area 332 stores an encryption key 425 which is a secret key used for decrypting the encrypted content 426 stored in the non-authentication area 331. The special area 304 stores

> the medium ID 341 which is necessary for accessing the authentication area 332. Hirota, col. 12, ll. 49-54.

The passage discloses an authentication area which stores an encryption key. However, absent from the cited passage is any teaching or suggestion that the authentication area is inaccessible in normal use.

The passage further discloses a special area which stores a medium ID. However, absent from the cited passage is any teaching or suggestion that the medium ID is equivalent to an encryption key.

The second passage cited by the Examiner states:

> The flash memory 303 is a flash-erasable, rewritable nonvolatile memory of a block deletion type, and includes logical storage areas: an authentication area 332 and a non-authentication area 331. The authentication area 332 can be accessed only by the apparatuses that have been authenticated as proper apparatuses. The non-authentication area 331 can be accessed by any apparatuses whether they are authenticated or not. In the present embodiment, the authentication area 332 is used for storing important data related to copyright protection, and the non-authentication area 331 is used as an auxiliary storage apparatus in a typical computer system. Note that a certain address in the flash memory 303 is used as a boundary between these two storage areas. Hirota, col. 10, ll. 22-36.

The cited passage discloses that the authentication area can be accessed only by apparatuses that have been authenticated as proper apparatuses. The Appellants respectfully submit that a storage area which can be accessed only by apparatuses that have been authenticated as proper apparatuses is not inherently equivalent to a storage area which is inaccessible in normal use. In particular, the accesses by “proper apparatuses” may constitute normal use.

Additional information about the authentication area (num. 332) disclosed by Hirota is disclosed in the following passage:

> It is therefore an object of the present invention to provide a semiconductor memory card that can be used as a storage medium for storing digital contents and as a storage medium for storing general-purpose computer data (not an object of copyright protection), and to provide an apparatus for reading data from the storage medium.

> The above object is fulfilled by a semiconductor memory card that can be used/removed in/from an electronic device, comprising: a rewritable nonvolatile memory; and a control circuit which controls accesses by the electronic device to an authentication area and a non-authentication area in the rewritable nonvolatile memory, wherein the control circuit includes: a nonauthentication area access control unit which controls accesses by the electronic device to the non-authentication area; an authentication unit which performs an authentication process to check whether the electronic device is proper, and affirmatively authenticates the electronic device when the electronic device is proper; and an authentication area access control unit which permits the electronic device to access the authentication area only when the authentication unit affirmatively authenticates the electronic device.
>
> With the above construction, the data being an object of copyright protection can be stored in the authentication area and other data can be stored in the non-authentication area, which makes it possible to achieve a semiconductor memory card which is capable of storing both digital contents to be copyright-protected and other data together. Hirota, col. 2, ll. 6-33.

The cited passage discloses that data being an object of copyright protection are stored in the authentication area disclosed in Hirota. Furthermore, the passage clearly states, "It is therefore an object of the present invention to provide . . . a storage medium for storing digital contents . . . ." Hirota, col. 2, ll. 6-8. It is thus evident that accessing the data being an object of copyright protection is central to the invention of Hirota. This suggests that accessing this data occurs during normal use. Because this data is stored in the authentication area, it follows that the authentication area disclosed by Hirota is accessed in normal use. The Appellants respectfully submit that because claim 3 requires the special storage area to be inaccessible in normal use, the authentication area of Hirota cannot be equivalent to the special storage area of claim 3.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 3. The Appellants submit that the rejection of claim 3 is in error and respectfully request that the rejection of claim 3 be reversed by the honorable Board.

III. CLAIM 4 IS NOT OBVIOUS OVER MATSUZAKI IN VIEW OF JOHNSON AND FURTHER IN VIEW OF JACKSON

Claim 4

Claim 4 is dependent on claim 1 and recites, "The data storage device according to claim 1, wherein the encryption circuit creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and the recording medium manages the storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys." It is emphasized that claim 4 requires the plurality of encryption keys to be created out of a plurality of personal identification information. Moreover, it is emphasized that claim 4 requires controlling user identification depending on each of the plurality of encryption keys.

The Examiner alleges that column 8, lines 33-47 of Jackson teach claim 4. FOA, pp. 12. The Examiner argues that the cited claim elements are found in Jackson by merely copying the claim elements and citing column and line numbers of Jackson in brackets. The rejection does not provide a comprehensive explanation of why the Examiner considers the limitations of claim 4 disclosed in Jackson. The Appellants respectfully submit that the Examiner has failed to clearly articulate a detailed explanation of disclosed structures relied upon in Jackson in accordance with 37 CFR 1.104(c)(2). Therefore, the Appellants respectfully submit that the Examiner has not met the burden of proof required to demonstrate obviousness.

The passage cited by the Examiner recites:

> CBC (and pipeline mode) require both a CV and an IV to be loaded in order to enable the drive. The IV would be a string of characters unique to the particular drive, perhaps including the serial number. The process is similar to that just described but an additional level of security is provided. In this case, the encryption algorithm for each sector of data will be based on the internal CV and an internal IV unique to the drive and that sector. This internal IV would be typically based on the input IV (itself depending on the drive serial number, for example) and on

> the logical block address of the sector in question. An advantage of this approach arises when identical data is written to each sector since the resulting encrypted data will differ sector by sector, making it more difficult to decode the encrypted data. Jackson, col. 8, ll. 33-47.

The Appellants respectfully submit that the cited passage fails to teach or suggest a plurality of encryption keys which is created out of a plurality of personal identification information as required by claim 4. The cited passage discloses a plurality of IV's. However, the passage fails to teach or suggest that the plurality of IV's are created out of a plurality of personal identification information. To the contrary, the passage teaches that the internal IV's (e.g., those specific to a sector) are calculated based on the logical block address of the sector with which the internal IV is associated and on an "input IV" which may depend on the drive serial number. It is evident that logical block addresses and drive serial numbers are not inherently equivalent to personal identification information.

Moreover, the Appellants respectfully submit that the cited passage fails to teach or suggest controlling user identification depending on each of the plurality of encryption keys as is required by claim 4.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 4. The Appellants submit that the rejection of claim 4 is in error and respectfully request that the rejection of claim 4 be reversed by the honorable Board.

IV. CLAIMS 7-12 AND 24 ARE NOT OBVIOUS OVER JACKSON IN VIEW OF JOHNSON

Claim 7

Claim 7 recites, in part, "wherein the encryption function of the control mechanism encrypts personal identification information by use of an encryption key created out of a given piece of the personal identification information." Thus, claim 7 requires encrypting personal identification information by use of an encryption key.

Furthermore, it is evident from antecedent basis that the personal identification information which is encrypted is the same personal identification information of which a given piece was used to create the encryption key.

The Examiner concedes, "Jackson is silent on the device wherein the encryption key is created out of a given piece of the personal identification information." FOA, pp. 13. However, the Examiner alleges that column 10, lines 48-65 of Johnson teaches creating an encryption key out of a given piece of personal identification information. FOA, pp. 13. The cited passage states:

> The step 804 of initializing the UAS 12 with recognition and comprehension data is shown in greater detail in FIG. 4b. As shown in FIG. 4b, processor 30 starts the data initialization process by prompting 810 the user for a dynamic personal identification number (DPIN) or code. This DPIN may be any desired alpha-numeric which the user wants to use as an identification code. Step 810 is preferably carried out by sending a user prompt to the display subsystem 50 and soliciting a response from the user via the keyboard subsystem 52. Once a DPIN is received from the keyboard subsystem 52, processor 30 proceeds to generate 814 a master hash code and a master key code using the DPIN as input. As will be explained later, this master key code is used to encrypt information stored on the master EKE 70. Preferably, processor 30 generates the master key code in two steps. First, processor 30 executes the hash code generation logic stored in section 62 of the non-volatile memory 38, using the DPIN as input, to generate a master hash code. Processor 30 preferably generates the master hash code by implementing a hashing algorithm. In the preferred embodiment . . . . Johnson, col. 10, ll. 46-66.

The Appellants submit that column 10, lines 48-65 of Johnson do not disclose encrypting personal identification information and creating an encryption key out of a piece of the personal identification information. As previously noted, claim 7 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the encryption key.

Furthermore, the Appellants respectfully submit that even assuming *arguendo* that it would be obvious to combine the teachings of Johnson within the system of Jackson, the combination nonetheless fails to teach or suggest encrypting personal identification information by use of an encryption key created out of a given piece

of the personal identification information as required by claim 7. Even if personal identification information is encrypted by use of an encryption key as allegedly disclosed by Jackson, and even if said encryption key is created out of a given piece of personal identification information as allegedly disclosed by Johnson, it does not inherently follow that the personal identification information which is encrypted is the same as the personal identification information out of which the encryption key is created. As previously noted, claim 7 requires that the personal identification information which is encrypted is the same as the personal identification information of which a given piece was used to create the encryption key.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 7. The Appellants submit that the rejection of claim 7 is in error and respectfully request that the rejection of claim 7 be reversed by the honorable Board.

Claim 8

Claim 8 is dependent on claim 7 and recites, "The hard disk device according to claim 7, wherein the control mechanism judges as to whether the data are encrypted or not upon reading the data out of the storage medium, and further decrypts the data when the data are encrypted." It is emphasized that claim 8 requires judging as to whether data are encrypted or not.

The Examiner alleges that page 11, paragraphs [0041]-[0042] of Jackson teaches the limitation introduced by claim 8. FOA, pp. 14. The passage cited by the Examiner recites:

> On a host read operation to read a file, the sequencer 2 will retrieve the encrypted file data from the disks 11 (via the VCM, spindle 9, motor 14 and read/write heads 13) and load it into the SRAM 1. From the SRAM the data is transferred in eight byte packets to the DED where it is decrypted. The plain text is then transferred back to the SRAM and is transferred to the host when the SRAM is full. Space is then made available in the SRAM. This process continues until the whole file has been read.

> On a host write operation, the plain text is transferred from the host to the SRAM 1 via the host interface 10 and sequencer 2. The data in the SRAM is transferred in eight byte packets to the DED 4 where it is encrypted. Once all the data in the SRAM has been encrypted, the sequencer 2 will transfer the cipher text from the SRAM to the disks 11. Space is made available in the SRAM. If more host data is available, it is transferred to the SRAM and the process is repeated. Jackson, para. [0041]-[0042].

The Appellants respectfully submit that the cited passage fails to teach or suggest judging as to whether data are encrypted or not as is required by claim 8.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 8. The Appellants submit that the rejection of claim 8 is in error and respectfully request that the rejection of claim 8 be reversed by the honorable Board.

Claims 9 and 10

Claim 9 and 10 are dependent on and further limit claim 7. Since the rejection of claim 7 is believed in error, the rejection of claims 9 and 10 are also believed in error for at least the same reasons as claim 7.

Claim 11

Claim 11 is dependent on claim 10 and recites, "The hard disk device according to claim 10, wherein the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys." It is emphasized that claim 11 requires the plurality of encryption keys to be created out of a plurality of personal identification information. Moreover, it is emphasized that claim 11 requires controlling user identification depending on each of the plurality of encryption keys.

It is well settled that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336, quoted with approval in KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007).

The Examiner alleges that column 8, lines 33-47 of Jackson teach claim 11. FOA, pp. 15. The Examiner argues that the cited claim elements are found in Jackson by merely copying the claim elements and citing column and line numbers of Jackson in brackets. The rejection does not provide a comprehensive explanation of why the Examiner considers the limitations of claim 11 disclosed in Jackson. The Appellants respectfully submit that the Examiner has failed to clearly articulate a detailed explanation of disclosed structures relied upon in Jackson in accordance with 37 CFR 1.104(c)(2). Therefore, the Appellants respectfully submit that the Examiner has not met the burden of proof required to demonstrate obviousness.

Moreover, the passage cited by the Examiner is recited above in regards to claim 4. The Appellants respectfully submit that the cited passage fails to teach or suggest a plurality of encryption keys which is created out of a plurality of personal identification information as required by claim 11 for the same reasons discussed above regarding claim 4. Furthermore, the Appellants respectfully submit that the cited passage fails to teach or suggest controlling user identification depending on each of the plurality of encryption keys as is required by claim 11.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 11. The Appellants submit that the rejection of claim 11 is in error and respectfully request that the rejection of claim 11 be reversed by the honorable Board.

Claim 12

Claim 12 is dependent on and further limits claim 7. Since the rejection of claim 7 is believed in error, the rejection of claim 12 is

also believed in error for at least the same reasons as claim 7.

Claim 24

Claim 24 is dependent on claim 7 and recites, "The hard disk device according to claim 7, wherein the control mechanism writes the data in the recording medium without encrypting the data when the encryption function is turned off."

The Examiner alleges that column 5, lines 19-34 of Jackson teaches the limitation introduced by claim 24. FOA, pp. 15. The passage cited by the Examiner recites:

> . . . read from, said at least one mass storage device; said drive control means including permanent security control means formed and arranged for restricting read/write access to said at least one mass storage device via said encryption/decryption means, for at least the data content of data files to be written thereto or read therefrom, and password-dependent security control means formed and arranged for receiving user input password data, comparing said user input password data with predetermined password data stored in said password-dependent security control means, and for activation of said encryption/decryption means only in response to receipt of a valid password, whereby read/write access to said at least one mass storage device, in relation to at least the data content of data files, is restricted to holders of a valid password. Jackson, col. 5, ll. 19-34 (para. [0020]).

The Appellants respectfully submit that the cited passage fails to teach or suggest writing the data in the recording medium without encrypting the data as required by claim 24.

Moreover, the Examiner argues that the cited claim elements are found in Jackson by merely copying the claim elements and citing column and line numbers of Jackson in brackets. The rejection does not provide a comprehensive explanation of why the Examiner considers the limitations of claim 24 disclosed in Jackson. The Appellants respectfully submit that the Examiner has failed to clearly articulate a detailed explanation of disclosed structures relied upon in Jackson in accordance with 37 CFR 1.104(c)(2). Therefore, the Appellants respectfully submit that the Examiner has not met the burden of proof required to demonstrate obviousness.

Furthermore, paragraph [0015] of Jackson states,

> Preferably, the encryption/decryption means is formed and arranged such that, in its deactivated state, no data can pass therethrough. Consequently, where the permanent security control means is adapted to route all data to be written to, or read from, the disk(s) through the encryption/decryption means, if the encryption/decryption means is in its deactivated state no data can be written to or read from the disk(s), whether in encrypted form or otherwise. Jackson, col. 4, ll. 19-27 (para. [0015]).

The Appellants respectfully submit that paragraph [0015] of Jackson teaches *away* from writing the data in the recording medium without encrypting the data when the encryption function is turned off as required by claim 24. Specifically, paragraph [0015] teaches that if the encryption/decryption means is in its deactivated state, no data can be written to or read from the disk(s). This suggests that if the encryption/decryption means in the passage cited by the Examiner is deactivated, no data can be written to the disks. Not writing data when the encryption/decryption means is deactivated is clearly not equivalent to writing the data in the recording medium without encrypting the data when the encryption function is turned off.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of obviousness for claim 24. The Appellants submit that the rejection of claim 24 is in error and respectfully request that the rejection of claim 24 be reversed by the honorable Board.

Conclusion

In view of the foregoing, Appellant submits that the rejections of claims 1-25 are improper and respectfully requests that the rejections of claims 1-25 be reversed by the Board.

Respectfully submitted,

Dated: July 1, 2008

/ido tuchman/

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
82-70 Beverly Road
Kew Gardens, NY 11415
Telephone (718) 544-1110
Facsimile (866) 607-8538

Claims Appendix

Claim 1. (original) A data storage device for an information processing device, the data storage device comprising:

an encryption circuit for encrypting desired data and personal identification information by use of an encryption key created out of a given piece of the personal identification information;

a recording medium for recording the data and the personal identification information encrypted by the encryption circuit; and

a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium.

Claim 2. (original) The data storage device according to claim 1,

wherein the encryption circuit encrypts the encryption key by use of a different encryption key, and

the recording medium records the encryption key encrypted by use of the different encryption key.

Claim 3. (original) The data storage device according to claim 1,

wherein the recording medium includes a special storage area which is inaccessible in normal use, and

the recording medium records the encryption key in the special storage area.

Claim 4. (original) The data storage device according to claim 1,

wherein the encryption circuit creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and

the recording medium manages the storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys.

Claim 5. (original) A data storage device for an information processing device, the data storage device comprising:

an encryption circuit for encrypting desired data by use of a first encryption key and for encrypting the first encryption key and personal identification information by use of a second encryption key created out of a given piece of the personal identification information;

a recording medium for recording the data encrypted by use of the first encryption key, the first encryption key encrypted by use of the second encryption key, and the personal identification information encrypted by use of the second key; and

a control unit for executing user verification by use of the encrypted personal identification information stored in the recording medium.

Claim 6. (original) The data storage device according to claim 5,

wherein the encryption circuit decrypts the encrypted first encryption key being read out of the recording medium by use of the second encryption key, and executes any of encryption and decryption of the desired data by use of the decrypted first encryption key.

Claim 7. (previously presented) A hard disk device comprising:

a magnetic disk being a recording medium;

a read-and-write mechanism for writing and reading data in and out of the magnetic disk; and

a control mechanism having an encryption function for encrypting data to be written in the magnetic disk and for decrypting the encrypted data to be read out of the magnetic disk, the control mechanism for

controlling reading and writing the data by the reading-and-writing mechanism,

wherein the control mechanism executes encryption of the data to be written in the magnetic disk for each unit of writing and reading data in and out of a storage area of the magnetic disk upon processing of writing the data in the magnetic disk, in response to turning on and off of the encryption mechanism, and

wherein the encryption function of the control mechanism encrypts personal identification information by use of an encryption key created out of a given piece of the personal identification information.

Claim 8. (original) The hard disk device according to claim 7,

wherein the control mechanism judges as to whether the data are encrypted or not upon reading the data out of the storage medium, and further decrypts the data when the data are encrypted.

Claim 9. (original) The hard disk device according to claim 7,

wherein the control mechanism decrypts the read-out data when the data read out of the recording medium are encrypted, and

the control mechanism encrypts and writes the data in the recording medium when the encryption function is turned on.

Claim 10. (previously presented) The hard disk device according to claim 7,

wherein the encryption function of the control mechanism encrypts desired data by use of the encryption key created out of a given piece of the personal identification information, and

the control mechanism executes user verification by use of the encrypted personal identification information.

Claim 11. (original) The hard disk device according to claim 10,

wherein the encryption function of the control mechanism creates a plurality of encryption keys out of a plurality of personal identification information and controls the user identification and the data encryption depending on each of the plurality of encryption keys, and

the magnetic disk manages storage areas in accordance with the plurality of keys, and records the encrypted data in the respective storage areas by use of the corresponding encryption keys.

Claim 12. (previously presented) The hard disk device according to claim 7,

wherein the encryption function of the control mechanism encrypts desired data by use of a first encryption key and encrypts the first encryption key by use of the encryption key created out of a given piece of the personal identification information, and

the control mechanism executes user verification by use of the encrypted personal identification information.

Claim 13. (previously presented) An information processing device comprising:

an operation control unit for executing various operation processing; and

a data storage device for storing data to be processed by the operation control unit,

wherein the data storage device includes an encryption function for encrypting desired data by use of a data encryption key and for encrypting personal identification information by use of a verification encryption key created out of a given piece of the personal identification information, and

the data storage device executes user verification by use of the encrypted personal identification information.

Claim 14. (original) The information processing device according to claim 13,

wherein the data encryption key and the verification encryption are mutually identical.

Claim 15. (original) The information processing device according to claim 13,

wherein the data storage device encrypts the data encryption key by use of a different encryption key and saves the encrypted data encryption key.

Claim 16. (original) The information processing device according to claim 15,

wherein the data storage device encrypts the data encryption key by use of the verification encryption key as the different encryption key.

Claim 17. (original) A data processing method for a data storage device for executing data writing and reading in and out of a recording medium of a data storage device, the data processing method for a data storage device comprising the steps of:

creating an encryption key out of a given piece of personal identification information;

encrypting the personal identification information by use of the encryption key and thereby recording the encrypted personal identification information in the recording medium as verification data;

executing user verification based on the verification data recorded in the recording medium; and

executing any of encrypting write data transmitted from a host system by use of the encryption key and thereby recording the encrypted write data in the recording medium, and, decrypting the data read out of the recording medium by use of the encryption key and thereby transmitting

the decrypted data to the host system.

Claim 18. (original) The data processing method for a data storage device according to claim 17, further comprising the steps of:

encrypting the encryption key by use of a different encryption key and thereby recording the encrypted encryption key in the recording medium; and

decrypting the encrypted encryption key by use of the different encryption key and thereby decrypting the data read out of the recording medium by use of the decrypted encryption key.

Claim 19. (original) A data processing method for a data storage device for executing data writing and reading in and out of a recording medium of a data storage device, the data processing method for a data storage device comprising the steps of:

creating a verification encryption key out of a given piece of personal identification information;

encrypting the personal identification information by use of the verification encryption key and recording the encrypted personal identification information in the recording medium as verification data, and further encrypting a data encryption key by use of the verification encryption key and thereby recording the encrypted data encryption key in the recording medium;

executing user verification based on the verification data recorded in the recording medium;

decrypting the data encryption key recorded in the recording medium by use of the verification encryption key; and

executing any of encrypting write data transmitted from a host system by use of the decrypted data encryption key and thereby recording the encrypted write data in the recording medium, and decrypting the data read out of the recording medium by use of the data encryption key and thereby transmitting the decrypted data to the host system.

Claim 20. (original) The data processing method for a data storage device according to claim 19, further comprising the step of:

decrypting the encrypted data encryption key recorded in the recording medium along with a change in the personal identification information by use of the verification encryption key created out of the personal identification information prior to the change, and then encrypting the data encryption key again by use of the verification encryption key created out of the personal identification information after the change and thereby storing the data encryption key in the recording medium.

Claim 21. (original) The data processing method for a data storage device according to claim 19, further comprising the step of:

decrypting the encrypted data encryption key recorded in the recording medium upon disabling encryption of the data recorded in the recording medium by use of the verification encryption key created out of the personal identification information prior to a change and thereby storing the decrypted data encryption key in the recording medium.

Claim 22. (previously presented) A program stored in computer readable memory for controlling a computer to control data writing and reading in and out of a magnetic disk, the program causing the computer to execute the processes of:

creating an encryption key out of a given piece of personal identification information;

encrypting the personal identification information by use of the encryption key and thereby recording the encrypted personal identification information in the magnetic disk as verification data;

executing user verification based on the verification data recorded in the magnetic disk; and

executing any of encrypting write data transmitted from a host

system by use of the encryption key and thereby recording the encrypted write data in the magnetic disk, and decrypting the data read out of the magnetic disk by use of the encryption key and thereby transmitting the decrypted data to the host system.

Claim 23. (previously presented) A program stored in computer readable memory for controlling a computer to control data writing and reading in and out of a magnetic disk, the program causing the computer to execute the processes of:

creating an verification encryption key out of a given piece of personal identification information;

encrypting the personal identification information by use of the verification encryption key and recording the encrypted personal identification information in the magnetic disk as verification data, and further encrypting a data encryption key by use of the verification encryption key and thereby recording the encrypted data encryption key in the magnetic disk;

executing user verification based on the verification data recorded in the magnetic disk;

decrypting the data encryption key recorded in the magnetic disk by use of the verification encryption key; and

executing any of encrypting write data transmitted from a host system by use of the decrypted data encryption key and thereby recording the encrypted write data in the magnetic disk, and decrypting the data read out of the magnetic disk by use of the data encryption key and thereby transmitting the decrypted data to the host system.

Claim 24. (previously presented) The hard disk device according to claim 7,

wherein the control mechanism writes the data in the recording medium without encrypting the data when the encryption function is turned off.

Claim 25. (previously presented) The data processing method of claim 17, wherein the user verification comprises:

creating a candidate encryption key out of a given piece of candidate personal identification information;

creating candidate verification data by encrypting the candidate personal identification information by use of the candidate encryption key; and

determining whether the candidate verification data are identical to the verification data previously recorded in the recording medium.

Evidence Appendix

None.

Related Proceedings Appendix

None.